

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. Where claims have been amended and/or canceled, such amendments and/or cancellations are done without prejudice and/or waiver and/or disclaimer to the claimed and/or disclosed subject matter, and Assignee reserves the right to claim this subject matter and/or other disclosed subject matter in a continuing application or otherwise.

1. (Currently Amended): An apparatus, comprising:

Management Frames utilized in wireless communications associated with said apparatus; and

said Management Frames being protection-capable or non-protection-capable and wherein said Management Frames indicate whether or not they are protection-capable based on a state of a Robust Security Network (RSN) Capabilities bit;

wherein if the state of said RSN Capabilities bit is set to protection-capable, said Management Action Frames are protected by applying an the IEEE 802.11i CCMP protocol -based encryption technique-construction to said protection-capable Management Action Frames.

2. (Currently Amended): The apparatus of claim 1, wherein at least one of said Management Frames comprises is an Action Frame.

3. (Currently Amended): The apparatus of claim 2, wherein said ~~wireless communications further comprises a Robust Security Network (RSN)~~ RSN Capabilities bit provides a protection negotiation capability to the ~~to be added for Action Frame protection negotiation.~~

4. (Currently Amended): The apparatus of claim 3, wherein said Action Frame protection negotiation is provided by a Beacon/Probe Response source setting the state of said RSN Capabilities bit to indicate that protection is required for all protection-capable Action Frames.

5. (Canceled)

6. (Currently Amended): The apparatus of claim 3, wherein if the state of said RSN Capabilities bit is set to protection-capable, said Action ~~Frame~~Frames ~~is~~are protected by applying ~~an~~the IEEE 802.11i TKIP protocol ~~based encryption technique~~construction to said protection-capable Action ~~Frame~~Frames.

7. (Currently Amended): The apparatus of claim 1, wherein said CCMP protocol-based encryption technique uses CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from modification.

8. (Currently Amended): The apparatus of claim 1, wherein said apparatus ~~comprises~~is a pair of Wireless stations (STA).

9. (Currently Amended): The apparatus of claim 8, wherein at least one of said pair of wireless stations (STA) ~~comprises~~is an access point (AP).

10. (Currently Amended): The apparatus of claim 6, wherein said TKIP protocol-based encryption technique uses RC4 to encrypt the Management Frame payload and uses Michael to protect selected Management Frame header fields from modification.

11. (Currently Amended): The apparatus of claim 6, wherein said apparatus comprises a pair of wireless stations (STA).

12. (Currently Amended): The apparatus of claim 11, wherein at least one of said wireless stations (STA) comprises an access point (AP).

13. (Currently Amended): The apparatus of claim 8, wherein one of the pair of STAs sourcing a Beacons and Probe Response, said STA sourcing Beacons and Probe Responses ~~sets~~ setting the state of the RSN Capabilities bit to 0 if said protected Management Action Frames are not supported/enabled; said STA sets and setting the state of the RSN Capabilities bit to 1 if said protected Management Action Frames are supported and enabled; the other of the pair of STAs responding by setting the state of the RSN Capabilities bit ~~said responding STA sets to 0 if the responding STA~~ it does not support protected Management Action Frames; and said responding STA setting the state of the RSN Capabilities bit to 1 ~~sets to the value set by said sourcing STA if the responding STA~~ it supports protected Management Action Frames.

14. (Currently Amended): The apparatus of claim 1, wherein said wireless communications comprises an 802.11-based wireless LAN.

15. (Currently Amended): A method of protecting Management Frames in wireless communications, comprising:

establishing said Management Frames as protection-capable or non- protection-capable; and

protecting said Management Frames if said Management Frames are protection-capable by;

~~wherein said step of protecting said Management Frames, comprises:~~

~~adding a Robust Security Network (RSN) Capabilities bit to said Management Frames for Management Frame protection negotiation based on a state of the RSN Capabilities bit, wherein if the state of said RSN Capabilities bit is set to protection-capable, said Management Frames are protected by applying an IEEE 802.11i CCMP protocol-based encryption technique a ~~protection protocol~~ to said protection-capable Management Frames; ~~wherein said protection protocol is the IEEE 802.11i CCMP protocol construction.~~~~

16. (Canceled)

17. (Currently Amended): The method of claim 15, wherein said Management Frame protection negotiation is provided by a Beacon/Probe Response source setting the state of said RSN bit to indicate that protection is required for all protection-capable Action Frames.

18. (Canceled)

19. (Currently Amended): The method of claim 15, wherein at least one of said Management Frames comprises ~~is~~ an Action Frame.

20. (Currently Amended): The method of claim 15, wherein if the state of said RSN Capabilities bit is set to protection-capable, said Management Frames are protected by applying an~~the~~ IEEE 802.11i TKIP protocol based encryption technique~~construction~~ to said protection-capable Management Action~~Action~~ Frames.

21. (Currently Amended): The method of claim 15, wherein said CCMP protocol based encryption technique uses CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from modification.

22. (Currently Amended): The method of claim 20, wherein said TKIP protocol based encryption technique uses RC4 to encrypt the Management Frame payload and uses Michael to protect selected Management Frame header fields from modification.

23. (Currently Amended): The method of claim 15, wherein said wireless communications comprises~~is~~ wireless communications between a pair of wireless stations (STA), one which comprises~~might be~~ an access point (AP).

24. (Currently Amended): The method of claim 23, wherein one of the pair of STAs comprising a~~said~~ sourcing STA that sets the state of the RSN Capabilities bit to 0 if said protected Management Frames are not supported/enabled; said sourcing STA setting the state of the RSN Capabilities bit~~sets~~ to 1 if said protected Management Frames are supported and enabled; the other of the pair of STAs responding by setting the state of the RSN Capabilities bit~~said STA sets~~ to 0 if the responding STA~~it~~ does not support protected Management Frames; and said responding STA setting the state of the RSN Capabilities bit to 1~~sets to value set by said AP if the responding STA~~~~it~~ supports protected Action Frames.

25. (Currently Amended): The method of claim 15, wherein said wireless communications ~~comprises~~ is an IEEE 802.11-based wireless LAN.

26. (Currently Amended): An article comprising a storage medium having stored thereon instructions, that, when executed by a computing platform, establishes, in a wireless communication environment, protection-capable and non-protection-capable Management Frames, said protection-capable Management Frames being protected;

wherein said protection-capable Management Frames ~~being protected~~ are protected by adding a Robust Security Network (RSN) Capabilities bit to said Management Frames for Management Frame protection negotiation based on a state of the RSN Capabilities bit, wherein if the state of said RSN Capabilities bit is set to protection-capable, said Management Frames are protected by applying an IEEE 802.11i CCMPa-protection protocol-based encryption technique for an IEEE 802.11i TKIP protocol-based encryption technique to said protection-capable Management Frames ~~wherein said protection protocol is the IEEE 802.11i CCMP or TKIP protocol construction.~~

27. (Canceled)

28. (Currently Amended): The article of claim 26, wherein said Management Frame protection negotiation is provided by a source of a Beacon/Probe Response ~~source~~ setting the state of said RSN Capabilities bit to indicate that protection is required for all protection-capable Action Frames.

29. (Canceled)

30. (Currently Amended): The article of claim 26, wherein at least one of said Management Frames comprises an Action Frame.

31. (Currently Amended): The article of claim 26, wherein said CCMP protocol-based encryption technique uses CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from modification, or uses the TKIP protocol-based encryption technique which uses RC4 to encrypt the Management Frame payload and Michael to protect selected Management Frame header fields from modification.

32. (Currently Amended): The article of claim 26, wherein said wireless communications comprises an IEEE 802.11-based wireless communications between a pair of wireless stations (STA), one of which comprises an access point (AP).

33. (Currently Amended): A system to protect Action Frames in Wireless LAN Communications, comprising:

a first wireless station (STA); and

a second STA in communication with said first STA, said communication comprising non-protection-capable Action Frames and protection-capable Action Frames;

wherein if the wireless communication requires protected Action Frames, then said first or said second STA discards any unprotected protection-capable Action Frame it receives, and wherein the discard of any unprotected protection-capable Action Frames includes those received before an IEEE 802.11i-based 4-Way Handshake completes.

34. (Currently Amended): The system of claim 33, wherein if it is desired not to protect Action Frames, then the first and second STAs ~~shall~~ send all Action Frames without protection, including all protection capable Action Frames.

35. (Currently Amended): The system of claim 33, wherein if it is desired to protect Action Frames, then a STA ~~protects~~~~shall protect~~ all protection-capable Action Frames, said protection provided by adding a Robust Security Network (RSN) Capabilities bit to said Action Frames for Action Frame protection negotiation, wherein if a state of said RSN Capabilities bit is set to protection-capable, said ActionManagement Frames are protected by applying a CCMP protocol-based encryption technique that ~~which~~ uses CCM to encrypt the ActionManagement Frame payload and to protect selected ActionManagement Frame header fields from modification, or by applying the TKIP protocol-based encryption technique that ~~which~~ uses RC4 to encrypt the ActionManagement Frame payload and Michael to protect selected ActionManagement Frame header fields from modification.

36. (Currently Amended): The system of claim 33, where said first STA ~~does~~~~shall~~ not send protection-capable Action Frames at all if said second STA has not agreed to protection.

37. (Canceled)

38. (Canceled)

39. (Currently Amended): The system of claim 33, wherein neither said first ~~nor~~ said second STA ~~shall attempt to protect non-protection-capable Action Frames the STA# sends~~ and ~~discards~~~~shall discard~~ any non-protection-capable Action Frames the STA# receives protected.

40. (Currently Amended): The system of claim 33, further comprising a third STA in communication with said second STA.